

(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES
PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro



(43) Internationales Veröffentlichungsdatum
27. März 2003 (27.03.2003)

PCT

(10) Internationale Veröffentlichungsnummer
WO 03/025714 A2

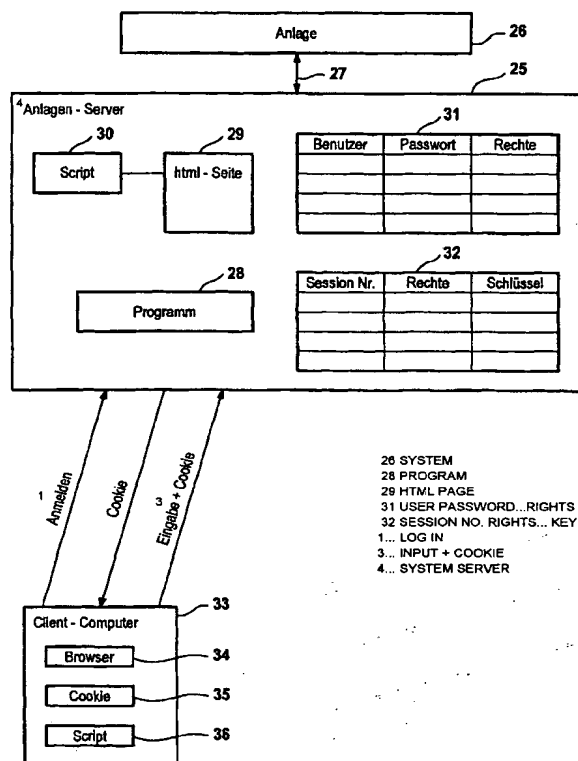
- (51) Internationale Patentklassifikation⁷: **G06F 1/00**
- (21) Internationales Aktenzeichen: **PCT/DE02/03105**
- (22) Internationales Anmeldedatum:
23. August 2002 (23.08.2002)
- (25) Einreichungssprache: **Deutsch**
- (26) Veröffentlichungssprache: **Deutsch**
- (30) Angaben zur Priorität:
101 44 336.6 10. September 2001 (10.09.2001) **DE**
- (71) Anmelder (für alle Bestimmungsstaaten mit Ausnahme von
US): **SIEMENS AKTIENGESELLSCHAFT [DE/DE];**
Wittelsbacherplatz 2, 80333 München (DE).

- (72) Erfinder; und
- (75) Erfinder/Anmelder (nur für US): **SCHLERETH, Michael [DE/DE];** Feld-Am-See-Ring 29, 91452 Wilhermsdorf (DE).
- (74) Gemeinsamer Vertreter: **SIEMENS AKTIENGESELLSCHAFT;** Postfach 22 16 34, 80506 München (DE).
- (81) Bestimmungsstaat (national): **US.**
- (84) Bestimmungsstaaten (regional): europäisches Patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SK, TR).

[Fortsetzung auf der nächsten Seite]

(54) Title: **SYSTEM SERVER COMPUTER AND METHOD FOR MONITORING THE INPUT RIGHTS OF A USER**

(54) Bezeichnung: **ANLAGEN-SERVER-COMPUTER UND VERFAHREN ZUR ÜBERPRÜFUNG DER RECHTE FÜR EINE EINGABE EINES BENUTZERS**



(57) Abstract: The invention relates to a computer system and to a method for monitoring the input rights of a user in relation to a system server computer (25), comprising the following steps: transmission of a cookie together with the input of a client computer (33) of the user to the system server computer (25), said cookie containing a key for access to the rights of the user; and monitoring the input rights of the user by means of a key.

(57) Zusammenfassung: Die Erfindung betrifft ein Computersystem und Verfahren zur Überprüfung der Rechte für eine Eingabe eines Benutzers in einen Anlagen-Server-Computer (25) mit folgenden Schritten: Übertragung eines Cookies zusammen mit der Eingabe von einem Client-Computer (33) des Benutzers an den Anlagen-Server-Computer (25), wobei der Cookie einen Schlüssel zum Zugriff auf Rechte des Benutzers beinhaltet, Überprüfung der Rechte des Benutzers für die Eingabe mittels des Schlüssels.

WO 03/025714 A2

**Erklärungen gemäß Regel 4.17:**

- hinsichtlich der Berechtigung des Anmelders, ein Patent zu beantragen und zu erhalten (Regel 4.17 Ziffer ii) für die folgenden Bestimmungsstaaten europäisches Patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SK, TR)
- Erfindererklärung (Regel 4.17 Ziffer iv) nur für US

Veröffentlicht:

- ohne internationalen Recherchenbericht und erneut zu veröffentlichen nach Erhalt des Berichts

Zur Erklärung der Zweibuchstaben-Codes und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

Beschreibung

Anlagen-Server-Computer und Verfahren zur Überprüfung der Rechte für eine Eingabe eines Benutzers

Die Erfindung betrifft ein Verfahren sowie einen Anlagen-Server-Computer und ein Computersystem zur Überprüfung der Rechte für eine Eingabe eines Benutzers von einem Client-Computer.

Aus dem Stand der Technik sind verschiedene Verfahren zur Authentifizierung eines Benutzers bekannt. Aus der US-A-6 205 480 ist ein System und Verfahren zur Benutzer-Authentifizierung gegenüber einem Webserver bekannt. Nach einer initialen Authentifizierungsprozedur wird die Identität des Benutzers in einer Genehmigungsdatei abgebildet, die eine Benutzerrolle beinhaltet und die als so genanntes Cookie gebildet ist. Für den Zugriff auf ein Anwendungsprogramm, das eine Authentifizierung erfordert, wird das Cookie einem Script zur Verfügung gestellt und die Information in dem Cookie wird zur Gewinnung von Authentifizierungsdaten, die von dem gewünschten Anwendungsprogramm gefordert werden, genutzt.

Es ist ebenso an sich aus dem Stand der Technik bekannt ein Steuerungssystem, beispielsweise eine speicherprogrammierbare Steuerung (SPS), mit einem Anlagen-Server zu verknüpfen, auf den ein Client-Computer zugreifen kann. Der Client-Computer kann von dem Server-Computer html-Seiten laden, beispielsweise um Prozesswerte auf einer Benutzerschnittstelle anzuzeigen. Die Verknüpfung zwischen einem Ausgabefeld der html-Seite und dem Prozesswert ist dabei beispielsweise mittels eines JAVA-Script oder mittels OCX (OLE Control Extension) fest programmiert.

Aus der US-A-6061603 ist ein System für den Fernzugriff auf ein Steuerungssystem über ein kommerzielles Kommunikations-

netz bekannt. Die Fig. 1 zeigt ein Blockdiagramm dieses vorbekannten Systems.

5 Zu dem System gehört ein Personal-Computer 8 mit einem Browser-Programm 10. Bei dem Browser 10 kann es sich um einen kommerziell erhältlichen Internet-Browser wie zum Beispiel Netscape Communication Navigator oder Microsoft Internet Explorer handeln. Das Browser-Programm 10 dient zum Zugriff auf eine so genannte Website 4 über das Internet 14 zur Anzeige
10 der Inhalte der Website 4 auf dem Monitor 12 des Personal-Computers 8 für einen Nutzer 2.

Die Website 4 beinhaltet ein Netzwerk-Interface 16 mit einer eindeutigen Internetadresse 18 sowie einen Server-Computer 20
15 und ein Anwendungsprogramm 22. Der Server-Computer 20 dient zur Interpretierung von HTTP-Protokollen und verwendet TCP/IP mittels TCP/IP Stack 24, um mit dem Netzwerk-Interface 16 und dem Anwendungsprogramm 22 zu interagieren. Dadurch wird der Datentransfer zwischen dem Anwendungsprogramm 22 und dem Nutzer 2 über das Internet 14 ermöglicht.
20

Das Anwendungsprogramm 22 liefert Daten von einem Steuerungssystem 6. Diese Daten können zur Überwachung der Steuerung durch den Nutzer 2 genutzt werden, da diese Daten mittels des
25 TCP/IP Stack 24 von der Website 4 über das Internet 14 zu dem Personal-Computer 8 des Nutzers 2 übertragen werden können. Dadurch wird auf dem Personal-Computer 8 eine Mensch-Maschine-Schnittstelle geschaffen.

30 Der Nutzer 2 kann eine Verbindung mit dem Internet 14 über einen so genannten Internet-Service-Provider herstellen und dann die Adresse der Website 4 in das Browser-Programm 10 eingeben. Der Nutzer 2 kann dann mittels des Browsers 10 beispielsweise eine Homepage der Website 4 lesen und von dort
35 Informationen abrufen. Aufgrund einer Eingabe des Nutzers 2 sendet der Browser 10 Kommandos an die Website 4, die das Anwendungsprogramm 22 nutzt, um Informationen, die von dem

Steuerungssystem 6 zur Verfügung gestellt werden, zur Anzeige zu bringen. Nachteilig bei diesen vorbekannten Systemen ist insbesondere, dass das Anwendungsprogramm 22 spezifisch für ein bestimmtes Steuerungssystem 6 programmiert sein muss und
5 keinerlei Flexibilität erlaubt.

Der Erfindung liegt die Aufgabe zu Grunde, ein verbessertes Verfahren sowie einen verbesserten Anlagen-Server-Computer und ein Computersystem zur Überprüfung der Rechte für eine
10 Eingabe eines Benutzers zu schaffen.

Die der Erfindung zu Grunde liegende Aufgabe ist mit den Merkmalen der unabhängigen Patentansprüche jeweils gelöst.

15 Bevorzugte Ausführungsformen der Erfindung sind in den abhängigen Ansprüchen angegeben.

Die Erfindung erlaubt eine effektive Authentifizierung und Überprüfung der Rechte für eine Eingabe eines Benutzers bei
20 Verwendung eines Client-Computers zum Bedienen, Beobachten und / oder Projektieren einer Anlage, wobei über ein Netzwerk, beispielsweise ein Intranet, Extranet oder Internet auf die Anlage bzw. deren Anlagen-Server-Computer zugegriffen wird.

25 Bei dem Client-Computer kann es sich um jede Art von elektronischem Gerät handeln, welches zum Laden einer Seite in einer Auszeichnungssprache, beispielsweise mittels des HTTP Protokolls über das Internet geeignet ist. Insbesondere kann es
30 sich bei dem Client-Computer um einen so genannten dünnen Client („thin client“) handeln, der als Bedienoberfläche einen Webbrowser verwendet. Ferner kann als Client-Computer auch ein mobiler Computer oder ein so genanntes Webpad verwendet werden. Ebenso ist die Verwendung eines Mobiltelefons
35 mit einem WAP-Browser als Client geeignet.

Ein besonderer Vorteil der Kommunikation mittels eines Internetprotokolls ist die Möglichkeit, eine so genannte Firewall vor dem Anlagen-Server-Computer zu installieren, um die Anlage vor nicht autorisiertem Zugriff zu schützen.

5

Ein weiter besonderer Vorteil der Erfindung ist, dass für die Benutzeridentifikation und die Rechte-Zuordnung eine Internetinfrastruktur verwendet werden kann.

10 In einer ersten Ausführungsform der Erfindung wird dazu beim ersten Anmelden des Benutzers auf dem Anlagen-Server-Computer anlagenseitig ein Cookie vergeben. Dieses Cookie wird zu dem Client-Computer übertragen und dort gespeichert. Bei jedem Zugriff auf den Anlagen-Server-Computer seitens des Client-
15 Computers wird das Cookie zu dem Anlagen-Server-Computer hin übertragen. Durch den Anlagen-Server-Computer wird das Cookie dann dahingehend überprüft, ob der Benutzer über ausreichende Rechte für seine Eingabe verfügt. Dazu wird das Cookie auf automatisierungsspezifische Benutzerrechte abgebildet.

20

In einer weiteren bevorzugten Ausführungsform der Erfindung wird eine erweiterte URL (Uniform Resource Locator) für die Benutzeridentifizierung und die Überprüfung der Rechte verwendet. Dazu wird bei einer ersten Anmeldung des Benutzers
25 auf dem Anlagen-Server-Computer zunächst eine Benutzerkennung vergeben.

Diese Benutzerkennung wird serverseitig gespeichert. Der Anlagen-Server-Computer erzeugt nach der Anmeldung des Benutzers und der Vergabe der Benutzerkennung eine clientspezifische Seite in einer Auszeichnungssprache, die von dem Client-Computer über das Internet geladen wird.

30

In der clientspezifischen Seite sind verschiedene Links enthalten, wobei die URLs der Links jeweils eine Erweiterung
35 enthalten. In dieser Erweiterung ist die Benutzerkennung codiert oder uncodiert hinterlegt. Wenn nun der Benutzer des

Client-Computers einen solchen Link auf clientspezifischen Seite auswählt, wird die entsprechende URL mit der Erweiterung zu dem Anlagen-Server-Computer übertragen. Serverseitig wird dann die Benutzeridentifikation mittels der in der Erweiterung beinhaltenen Kennung vorgenommen und anhand der Erweiterung geprüft, ob der Benutzer für die Eingabe berechtigt ist. Dies erlaubt dem Benutzer eine anlagenspezifische Sicht anzubieten, die auf die Rechte, über die der Benutzer verfügt, abgestimmt ist.

Im Weiteren wird ein bevorzugtes Ausführungsbeispiel mit Bezugnahme auf die Zeichnungen näher erläutert. Es zeigen

Fig. 1 ein Blockdiagramm eines aus dem Stand der Technik bekannten Steuerungssystems,

Fig. 2 ein Blockdiagramm einer ersten Ausführungsform eines erfindungsgemäßen Computersystems,

Fig. 3 ein Flussdiagramm für die Anmeldung eines Benutzers auf dem Anlagen-Server-Computer des Computersystems der Fig. 2,

Fig. 4 ein Flussdiagramm für die Überprüfung der Rechte für eine Eingabe des Benutzers in dem Computersystem der Fig. 2,

Fig. 5 eine zweite bevorzugte Ausführungsform eines erfindungsgemäßen Computersystems, bei dem eine Erweiterung der URLs zur Überprüfung der Rechte verwendet wird,

Fig. 6 ein Flussdiagramm für die Anmeldung eines Benutzers und die Überprüfung der Rechte in dem Computersystem der Fig. 5.

Die Fig. 2 zeigt ein Computersystem mit einem Anlagen-Server-Computer 25 zur Überwachung, Steuerung und / oder Projektie-

5 rung einer Anlage 26. Der Anlagen-Server-Computer 25 kommuniziert mit der Anlage 26, bzw. mit einer speicherprogrammierbaren Steuerung der Anlage 26 oder mit verschiedenen Aggregaten der Anlage 26 über einen Feldbus 27.

10 Der Anlagen-Server-Computer 25 beinhaltet ein Computerprogramm 28 sowie eine Seite 29 in einer Auszeichnungssprache. Bei der Auszeichnungssprache kann es sich beispielsweise um die Hypertext Mark Up Language (HTML) oder um die Extended Hypertext Mark Up Language (XML) handeln. Auf der Seite 29 ist ein Script 30 codiert. Dabei kann es sich beispielsweise um ein JAVA Script handeln. Alternativ kann auch ein so genanntes Applet in der Seite 29 codiert sein.

15 In einer bevorzugten Ausführungsform ist das Script überflüssig, da das Cookie Handling in den Browser integriert ist. Vor jedem Zugriff auf einen Server überprüft der Browser, ob in seinem Speicher (z.B. Festplatte, RAM) ein Cookie für diesen Server vorhanden ist und überträgt den Inhalt des Cookies automatisch mit dem Seitenrequest an den Server).

20 Des Weiteren ist auf dem Anlagen-Server-Computer eine Tabelle 31 abgelegt, die jedem registrierten Benutzer ein Passwort sowie anlagenspezifische Zugriffsrechte zuordnet. Neben einem Passwort können auch andere Authentifizierungsmerkmale wie z.B. die ID einer Chipkarte eingesetzt werden. In diesem Fall würde die entsprechende ID des verwendeten Identifizierungsverfahrens hinterlegt werden.

30 Je nach der Rolle des betreffenden Benutzers können sich diese Rechte beispielsweise auf die Überwachung der Anlage, das heißt, die Anzeige von bestimmten Parameterwerten oder Abläufen beschränken, ohne dass Veränderungen vorgenommen werden dürfen. Auf der anderen Seite können die Rechte die Einstellung von Maschinenparametern und / oder die Vornahme von Wartungsarbeiten mit beinhalten.

Ferner ist auf dem Anlagen-Server-Computer 25 eine Tabelle 32 abgebildet. Die Tabelle 32 beinhaltet für jede aktive Verbindung zwischen einem Client-Computer eines der Benutzer und dem Anlagen-Server-Computer 25 eine separate Session, die
5 durch eine Sessionnummer identifiziert ist. Dabei werden jeder Sessionnummer die Rechte des Benutzers zugeordnet, sowie ein Cookie mit einem der Sessionnummer zugeordneten Schlüssel. Dieser Schlüssel ist in dem Cookie auf Client gespeichert. Das Cookie ist z.B. beim Internetexplorer eine Textdatei auf der Festplatte.
10

Das Computersystem beinhaltet ein oder mehrere Client-Computer 33, die über ein Netzwerk, beispielsweise das Internet, mit dem Anlagen-Server-Computer 25 kommunizieren können.
15 In dem gezeigten Ausführungsbeispiel der Fig. 2 ist lediglich ein Client-Computer 33 online mit dem Anlagen-Server-Computer 25.

Der Client-Computer 33 beinhaltet ein Browserprogramm 34 für den Zugriff auf Seiten in einer Auszeichnungssprache auf dem Anlagen-Server-Computer sowie für die Interpretation von Scripten. Hierbei kann es sich um einen üblichen Browser, wie z. B. Netscape Navigator oder Microsoft Internet Explorer, handeln.
20

Zum Aufbau einer Internetverbindung zwischen dem Client-Computer 33 und dem Anlagen-Server-Computer 25 gibt der Benutzer des Client-Computer 33 die URL der Seite 29 in das Browserprogramm 34 ein. Die Seite 29 mit dem Script 30 wird
30 dann von dem Anlagen-Server-Computer 25 zu dem Client-Computer 33 übertragen und dort mittels des Browserprogramms 34 angezeigt; das Script 30 wird von dem Browserprogramm 34 interpretiert und ausgeführt.

35 Zunächst wird der Benutzer des Client-Computers 33 dann zur Anmeldung auf dem Anlagen-Server-Computer 25, das heißt, zur

Eingabe seiner Benutzerkennung und seines Passworts aufgefordert.

Das Programm 28 des Anlagen-Server-Computers 25 prüft dann,
5 ob ein Benutzer mit dieser Benutzerkennung in der Tabelle 31
vorhanden ist und ob das eingegebene Passwort korrekt ist.
Ist dies der Fall, so vergibt das Programm 28 eine Sessionnummer
für die aktuelle Verbindung des Client-Computers 33 mit
dem Anlagen-Server-Computer 25 in der Tabelle 32.

10 Ferner greift das Programm 28 auf die Tabelle 31 zu, um die
Rechte des Benutzers zu ermitteln. Diese Rechte werden in der
Tabelle 32 unter der entsprechenden Sessionnummer abgespei-
chert. Ferner erzeugt das Programm 28 einen Cookie, der einen
15 Schlüssel für den Zugriff auf die in der Tabelle 32 abgespei-
cherten Rechte der betreffenden Sessionnummer beinhaltet.

Dieser Cookie wird dann von dem Anlagen-Server-Computer 25 zu
dem Client-Computer 33 übertragen und dort vom Browser in ei-
nem Speicher 35 des Client-Computers 33 abgelegt. Bei dem
20 Speicher 35 kann es sich beispielsweise um eine Festplatte
oder um einen anderen flüchtigen oder nicht flüchtigen Spei-
cher des Client-Computers 33 handeln.

25 Wenn der Benutzer des Client-Computers 33 eine Eingabe auf
der mittels des Browserprogramms 34 angezeigten Seite 29 vor-
nimmt und die Eingabetaste betätigt, wird die entsprechende
Eingabe an den Anlagen-Server-Computer 25 übertragen. Gleich-
zeitig sorgt der Browser, dafür, dass der Cookie aus dem
30 Speicher 35 gelesen wird und zusammen mit der Eingabe an den
Anlagen-Server-Computer 25 übertragen wird. Das Programm 28
liest dann den Schlüssel aus dem Cookie und greift mittels
des Schlüssels in der Tabelle 32 auf die Rechte des Benutzers
zu.

35 Das Programm 28 prüft dann, ob die Rechte des Benutzers für
die Eingabe ausreichend sind. Ist dies der Fall, wird die

Eingabe akzeptiert und gegebenenfalls über den Feldbus 27 an die Anlage 26 übertragen; im gegenteiligen Fall wird die Eingabe abgelehnt und der Benutzer erhält einen entsprechenden Hinweis.

5

Die Fig. 3 zeigt ein Flussdiagramm für die Anmeldung eines Benutzers - beispielsweise auf dem Anlagen-Server-Computer 25 der Fig. 2.

10 In dem Schritt 40 lädt der Benutzer eine Seite in einer Auszeichnungssprache, beispielsweise eine html-Seite. Der Benutzer erhält dann die Aufforderung zur Eingabe seiner Benutzerkennung und seines Passworts.

15 In dem Schritt 41 erfolgt dann serverseitig Zugriff auf eine Datenbank, in der sämtliche Benutzerkennungen der registrierten Benutzer sowie die entsprechenden Passworte und die den Benutzerkennungen zugeordneten Zugriffsrechte gespeichert sind.

20

In dem Schritt 42 wird geprüft, ob der Benutzer mit der eingegebenen Benutzerkennung in der Datenbank vorhanden ist und ob gegebenenfalls das Passwort oder eine andere Authentifizierung wie z.B. eine eingelegte Chipkarte korrekt ist. Ist dies nicht Fall, so erfolgt in dem Schritt 43 eine Zugriffsverweigerung.

25

Im gegenteiligen Fall wird in dem Schritt 44 eine Session für den Benutzer mit einer Sessionnummer erzeugt. Dazu werden die Benutzerrechte mit der Benutzerkennung als Schlüssel aus der Datenbank gelesen und zusammen mit der Sessionnummer in einer Tabelle gespeichert. Ferner wird ein Sessionschlüssel generiert, der zum Zugriff auf die Benutzerrechte der betreffenden Session in der Tabelle dient. Dieser Sessionschlüssel wird in einem Cookie gespeichert.

30

35

In dem Schritt 45 wird der Cookie an den Client-Computer des Benutzers übertragen und in dem Schritt 46 dort abgespeichert.

5 Die Fig. 4 zeigt den entsprechenden Vorgang bei der Eingabe eines Benutzers. In dem Schritt 50 erfolgt zunächst eine Eingabe des Benutzers auf der Seite, die zuvor in dem Schritt 40 (vgl. Fig. 3) geladen worden ist. Nach der Betätigung der Eingabetaste durch den Benutzer wird der entsprechende Eingabewert an den Anlagen-Server-Computer übertragen; gleichzeitig
10 sorgt der Browser dafür, dass auch das Cookie (vgl. Schritt 46 der Fig. 3) von dem betreffenden Speicher des Client-Computers gelesen und zu dem Anlagen-Server-Computer mit übertragen wird.

15

In dem Schritt 51 erfolgt ein Zugriff auf die Benutzerrechte in der Tabelle (vgl. Schritt 44 der Fig. 3), wobei für den Zugriff, der in dem Cookie codierte Schlüssel verwendet wird.

20 In dem Schritt 52 wird dann geprüft, ob die Rechte des Benutzers für die Eingabe ausreichend sind. Ist dies nicht der Fall, so erfolgt in dem Schritt 53 die Ablehnung dieser Eingabe. Im gegenteiligen Fall wird in dem Schritt 54 die Eingabe angenommen, von dem Anlagen-Server-Computer verarbeitet
25 und gegebenenfalls an die Anlage übertragen.

Von besonderem Vorteil bei dieser Ausführungsform ist, dass die Speicherung und Übertragung des Cookies für den Benutzer unsichtbar erfolgt und der Benutzer auf den Cookie und den
30 darin beinhaltenen Schlüssel keinen unmittelbaren Zugriff hat und den Cookie nicht zu anderen Benutzern weiter verbreiten kann. Damit ist eine weitere Schutzfunktion gegen unautorisierte Zugriffe gegeben.

35 Die Fig. 5 zeigt das Blockdiagramm einer weiteren bevorzugten Ausführungsform, in der Elemente, die Elementen der Fig. 2

entsprechen, mit den selben Bezugszeichen gekennzeichnet sind.

5 Im Unterschied zu der Ausführungsform der Fig. 2 ist auf dem Anlagen-Server-Computer 25 der Fig. 5 eine Tabelle 37 abgebildet, die für jeden registrierten Benutzer eine Benutzerkennung sowie ein entsprechendes Passwort und die der Benutzerkennung zugeordneten Rechte beinhaltet. Für die Anmeldung auf dem Anlagen-Server-Computer 25 muss der Benutzer wiederum
10 seine Benutzerkennung und sein Passwort eingeben.

Nach dieser Anmeldung wird von dem Programm 28 für die betreffende Session eine weitere Benutzerkennung (Benutzer ID) vergeben, die ebenfalls in der Tabelle 37 abgebildet
15 wird. Diese Benutzer ID ist der Benutzerkennung zugeordnet und dient als Schlüssel für den Zugriff auf die entsprechenden Rechte des betreffenden Benutzers. Diese dynamische Benutzer ID ist nur für die Zeitdauer einer Session gültig und kann nach dem Ende einer Session nicht mehr verwendet werden.
20

Das Programm 28 erzeugt dann dynamisch für den betreffenden Benutzer eine Seite 29 in einer Auszeichnungssprache. In der Seite 29 werden dem Benutzer verschiedene Links - bei der Verwendung einer Internetinfrastruktur, so genannte Hyper-
25 textlinks - z. B. Link 1, Link 2, Link 3 - jeweils für den Aufruf weiterer Seiten des auf dem Anlagen-Server-Computer 25 gespeicherten Webs angeboten. Die auf der Seite 29 für den Benutzer generierten Links können dabei entsprechend der Rechte des Benutzers von dem Programm 28 selektiert werden,
30 dass heißt, ein Benutzer mit geringeren Rechten erhält auch nur die seinen Rechten entsprechenden Links zur Auswahl.

Jeder der Links besteht aus einer URL, die eine Erweiterung beinhaltet. Diese Erweiterung kann beispielsweise an die URL
35 angehängt sein. Die Erweiterung beinhaltet die Benutzer ID.

Die dynamisch erzeugte Seite 29 wird von dem Anlagen-Server-Computer 25 zu dem Client-Computer 33 übertragen und dort mittels des Browsers 34 angezeigt.

5 Der Benutzer wählt dann einen der auf der Seite 29 angebotenen Links für den Aufruf einer weiteren Seite aus, beispielsweise durch einen so genannten Doppelklick auf den Link 1. Die betreffende Seite mit der URL des Link 1 wird dann auf den Client-Computer 33 geladen und mittels des Browsers 34
10 angezeigt. Der Benutzer des Client-Computers 33 kann dann auf dieser Seite mit der URL des Link 1 eine Eingabe vornehmen. Durch die Betätigung der Eingabetaste wird diese zusammen mit der URL und deren Erweiterung an den Anlagen-Server-Computer 25 übertragen. Das Programm 28 prüft dann aufgrund der in der
15 Erweiterung der URL beinhalteten Benutzer ID durch Zugriff auf die Tabelle 37, ob die entsprechenden Rechte des Nutzers für die Vornahme der Eingabe ausreichend sind.

Die Fig. 6 zeigt ein entsprechendes Flussdiagramm.
20

In dem Schritt 60 meldet sich der Benutzer zunächst auf dem Anlagen-Server-Computer an. In dem Schritt 61 wird dem Benutzer eine Benutzer ID serverseitig zugeordnet. Diese Benutzer ID dient als Schlüssel für den Zugriff auf die Benutzerrechte,
25 te, die auf dem Anlagen-Server-Computer hinterlegt sind.

In dem Schritt 62 wird dann dynamisch eine Seite in einer Auszeichnungssprache für den Benutzer generiert. Diese Seite beinhaltet Links, deren URL um die Benutzer ID erweitert ist.
30 Diese dynamisch erzeugte Seite wird in dem Schritt 63 von dem Client geladen und mittels eines Browserprogramms angezeigt. In dem Schritt 64 wählt der Benutzer einen der Links auf der Seite aus, so dass die entsprechende Seite geladen wird und mittels des Browserprogramms auf dem Client-Computer ange-
35 zeigt wird.

In dem Schritt 65 tätigt der Benutzer eine Eingabe auf der Seite mit dem in dem Schritt 64 ausgewählten Link. Bei Betätigung der Eingabetaste wird diese Eingabe zusammen mit der erweiterten URL der Seite zu dem Anlagen-Server-Computer übertragen, wo in dem Schritt 65 eine Überprüfung der Rechte des Benutzers erfolgt. Dazu wird mit der Benutzer ID, die in der Erweiterung der URL des Links der betreffenden Seite beinhaltet ist, als Schlüssel auf die Rechte des Benutzers zugegriffen, um zu prüfen, ob diese für die Vornahme der Eingabe ausreichend sind.

Wenn das Ergebnis der Entscheidung in dem Schritt 66 ist, dass die Rechte nicht ausreichend sind, erfolgt in dem Schritt 67 eine Ablehnung dieser Eingabe.

Im gegenteiligen Fall erfolgt in dem Schritt 68 eine Annahme und Verarbeitung der Eingabe durch den Anlagen-Server-Computer.

Zusammenfassend betrifft die Erfindung ein Computersystem und Verfahren zur Überprüfung der Rechte für eine Eingabe eines Benutzers in einen Anlagen-Server-Computer mit folgenden Schritten:

- Übertragung eines Cookies zusammen mit der Eingabe von einem Client-Computer des Benutzers an den Anlagen-Server-Computer, wobei der Cookie einen Schlüssel zum Zugriff auf Rechte des Benutzers beinhaltet,
- Überprüfung der Rechte des Benutzers für die Eingabe mittels des Schlüssels.

Patentansprüche

1. Verfahren zur Überprüfung der Rechte für eine Eingabe eines Benutzers in einen Anlagen-Server-Computer (25) mit folgenden Schritten:

- Übertragung eines Cookies zusammen mit der Eingabe von einem Client-Computer (33) des Benutzers an den Anlagen-Server-Computer (25), wobei der Cookie einen Schlüssel zum Zugriff auf Rechte des Benutzers beinhaltet,
- Überprüfung der Rechte des Benutzers für die Eingabe mittels des Schlüssels.

2. Verfahren zur Überprüfung der Rechte für die Eingabe eines Benutzers in einen Anlagen-Server-Computer (25) mit folgenden Schritten:

- Lesen der Rechte des Benutzers aus einer ersten Datenbank (32) des Anlagen-Server-Computers (25),
- Erzeugung eines Cookies mit einem Schlüssel zum Zugriff auf die Rechte,
- Speicherung des Schlüssels,
- Übertragung des Cookies an den Client-Computer (33) des Benutzers,
- Übertragung des Cookies von dem Client-Computer (33) des Benutzers zusammen mit der Eingabe,
- Überprüfung der Rechte mittels des Schlüssels.

3. Verfahren nach Anspruch 1 oder 2, bei dem das Cookie bei einer Anmeldung des Benutzers auf dem Anlagen-Server-Computer

(25) erzeugt wird und die Zuordnung von Rechten zu dem Cookie in einer zweiten Datenbank (31) abgelegt wird.

5 4. Verfahren nach Anspruch 1, 2 oder 3, bei dem mit der Übertragung jeder Eingabe von dem Client-Computer (33) an den Anlagen-Server-Computer (25) das Cookie zur Überprüfung der Rechte für die betreffende Eingabe mit übertragen wird.

10 5. Verfahren nach einem der vorhergehenden Ansprüche 1 bis 4, bei dem eine Seite in einer Auszeichnungssprache von dem Anlagen-Server-Computer (25) auf den Client-Computer (33) geladen wird und ein Cookie im Seitenkopf übertragen wird.

15 6. Verfahren zur Überprüfung der Rechte für eine Eingabe eines Benutzers in einen Anlagen-Server-Computer (25) mit folgenden Schritten:

20 - Laden einer dynamisch erzeugten Seite mit einer URL mit einer Erweiterung, wobei die Erweiterung einen Schlüssel zum Zugriff auf Rechte des Benutzers beinhaltet,

- Vornahme einer Eingabe durch den Benutzer auf der Seite,

25 - Überprüfung der Rechte des Benutzers für die Eingabe mittels des in der Erweiterung beinhalteten Schlüssels.

30 7. Verfahren zur Überprüfung der Rechte für eine Eingabe eines Benutzers in einen Anlagen-Server-Computer (25) mit folgenden Schritten:

- Zuordnung eines Schlüssels zu dem Benutzer,

- Speicherung des Schlüssels,

35 - dynamische Erzeugung einer Seite in einer Auszeichnungssprache mit einer URL mit einer Erweiterung, wobei die Erweiterung den Schlüssel beinhaltet,

- Auswahl der URL durch den Benutzer und Vornahme einer Eingabe auf der zu der URL gehörenden Seite,

5 - Überprüfung der Rechte des Benutzers für die Eingabe mittels des Schlüssels,

8. Verfahren nach Anspruch 6 oder 7, bei dem bei der dynamischen Erzeugung der Seite in der Auszeichnungssprache mehrere URLs für weitere Seiten erzeugt werden und wobei jede der
10 URLs eine Erweiterung mit dem Schlüssel aufweist.

9. Anlagen-Server-Computer (25) mit

15 - einer ersten Datenbank (32) zur Zuordnung eines Schlüssels zu Rechten eines Benutzers,

- Mitteln (28) zum Empfang eines Cookies mit dem Schlüssel zusammen mit einer Eingabe,

20 - Mitteln (28) zum Zugriff auf die erste Datenbank (32) zur Überprüfung der Rechte des Benutzers für die Eingabe.

10. Anlagen-Server-Computer (25) nach Anspruch 9 mit einer zweiten Datenbank (31) für die Speicherung von verschiedenen Benutzern zugeordneten Rechten.
25

11. Anlagen-Server-Computer (25) nach Anspruch 9 oder 10 mit einer Seite (29) in einer Auszeichnungssprache mit einem Script (30) oder Applet, welches zur Übertragung des Cookies von einem Client-Computer (33) zu dem Anlagen-Server-Computer (25) zusammen mit der Eingabe dient.
30

12. Computersystem mit einem Anlagen-Server-Computer (25) nach einem der Ansprüche 9, 10 oder 11 und mit einem Client-Computer (33) eines Benutzers.
35

13. Anlagen-Server-Computer (25) mit

- Mitteln (37) zur Zuordnung einer Benutzerkennung als Schlüssel für den Zugriff auf Rechte des Benutzers,
- Mitteln (28) zur dynamischen Erzeugung einer Seite in einer Auszeichnungssprache mit einer URL mit einer Erweiterung, wobei die Erweiterung den Schlüssel beinhaltet.

14. Anlagen-Server-Computer (25) nach Anspruch 13, bei dem die Mittel (28) zur dynamischen Erzeugung einer Seite in einer Auszeichnungssprache zur Erzeugung von mehreren URLs für verschiedene weitere Seiten ausgebildet sind, wobei die URLs jeweils die Erweiterung aufweisen.

15. Anlagen-Server-Computer (25) nach Anspruch 13 oder 14 mit Mitteln zur Überprüfung einer Eingabe eines Benutzers von einer Seite mit einer der URLs mit der Erweiterung durch Zugriff auf die Rechte mittels des Schlüssels.

1 / 6

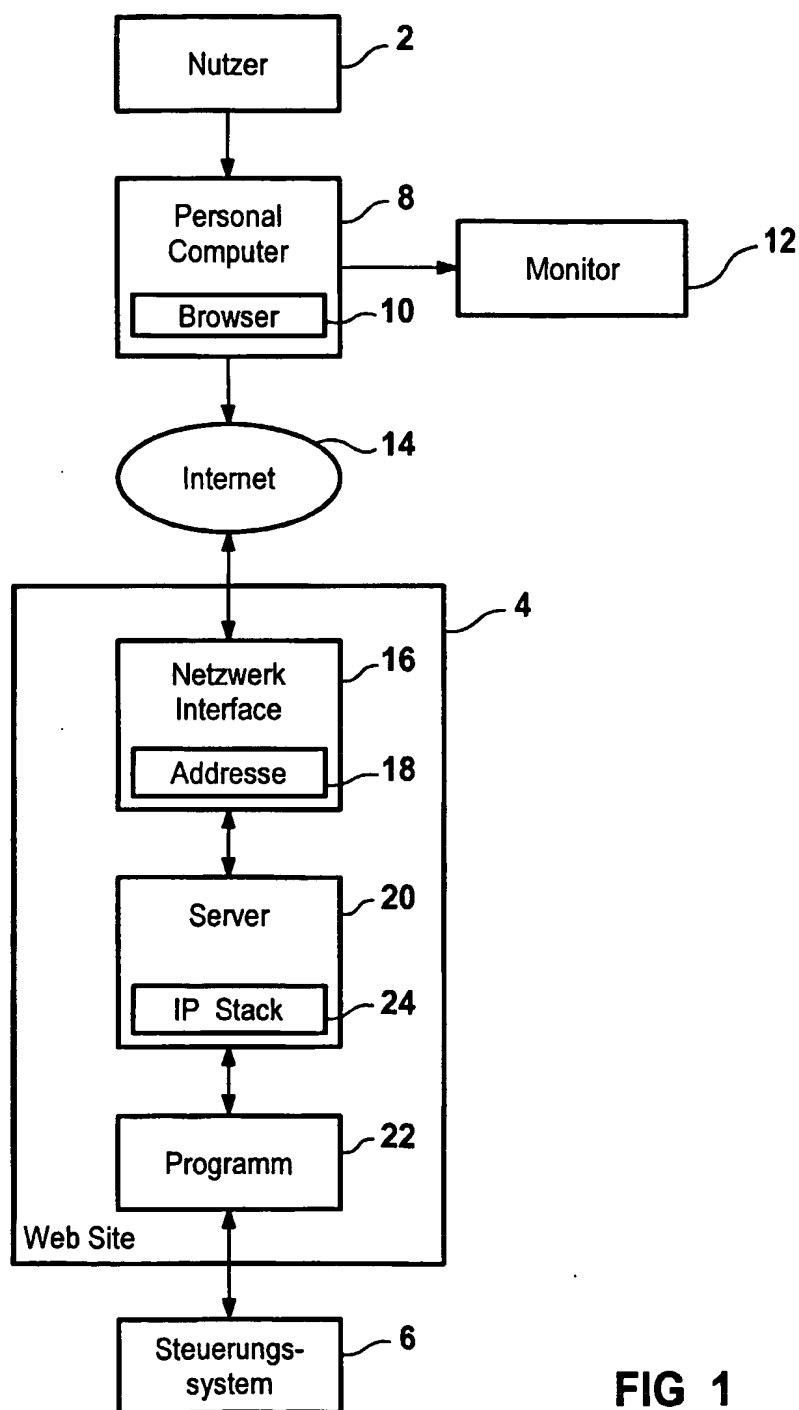


FIG 1

2 / 6

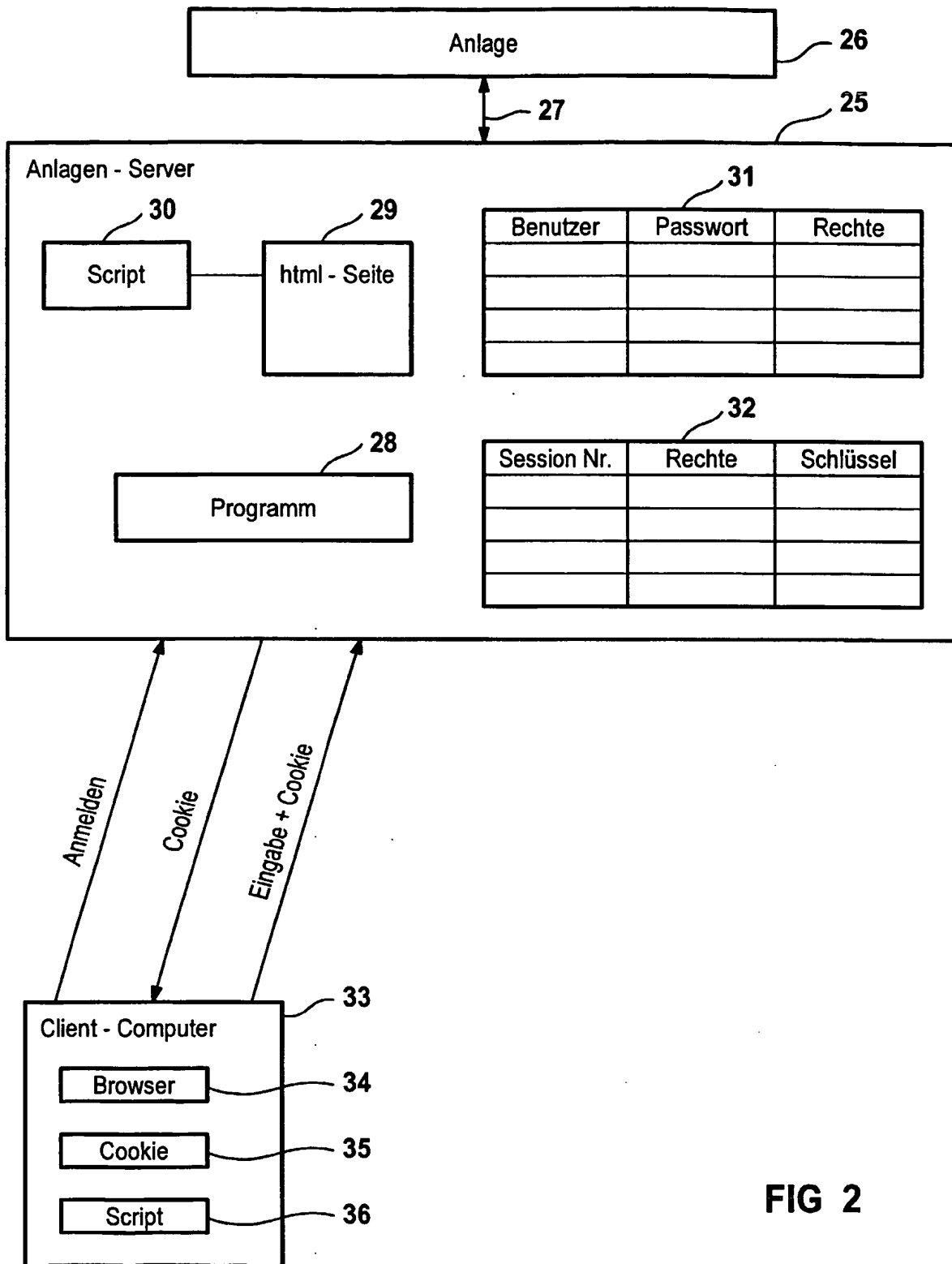


FIG 2

3 / 6

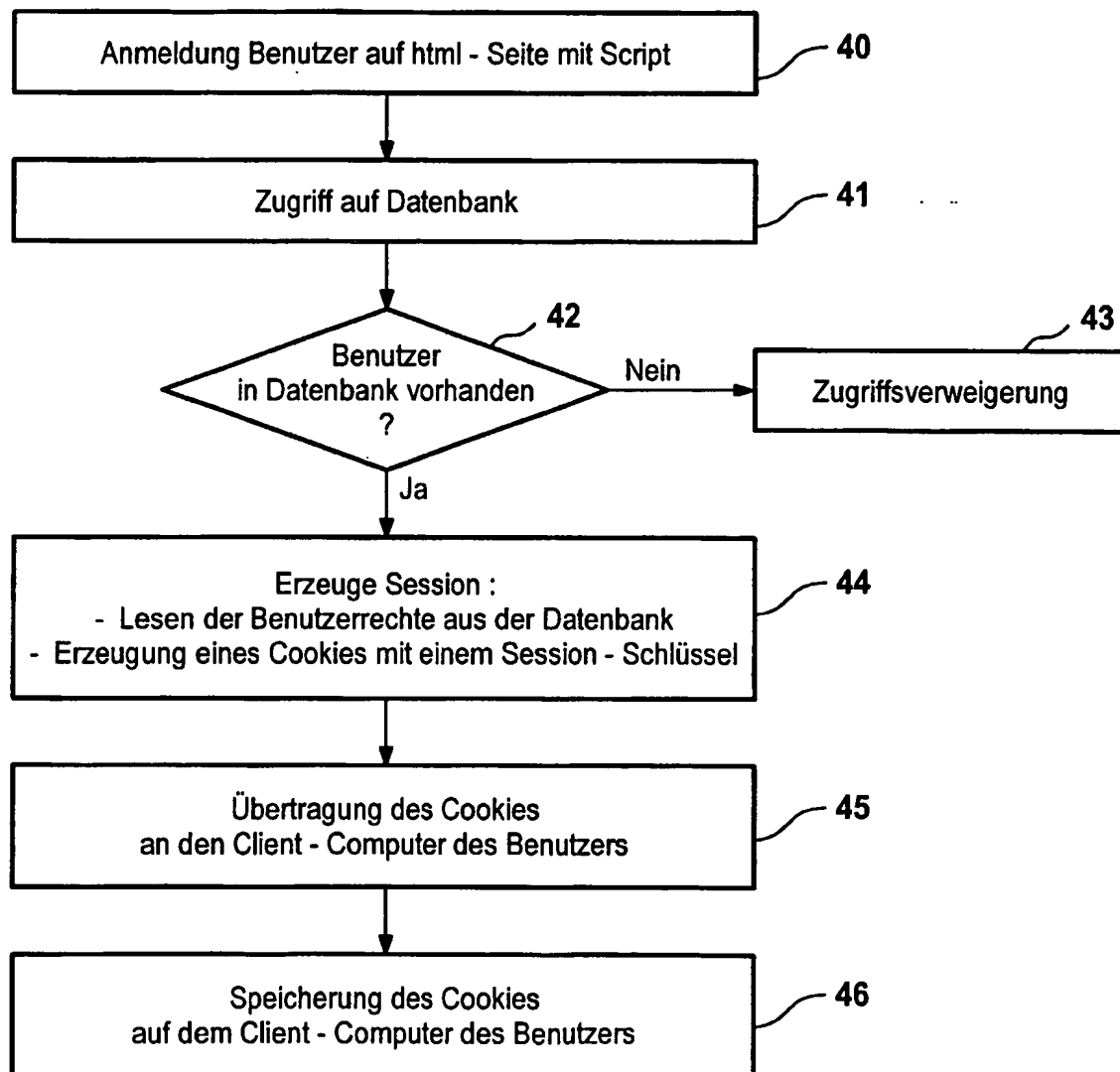


FIG 3

4 / 6

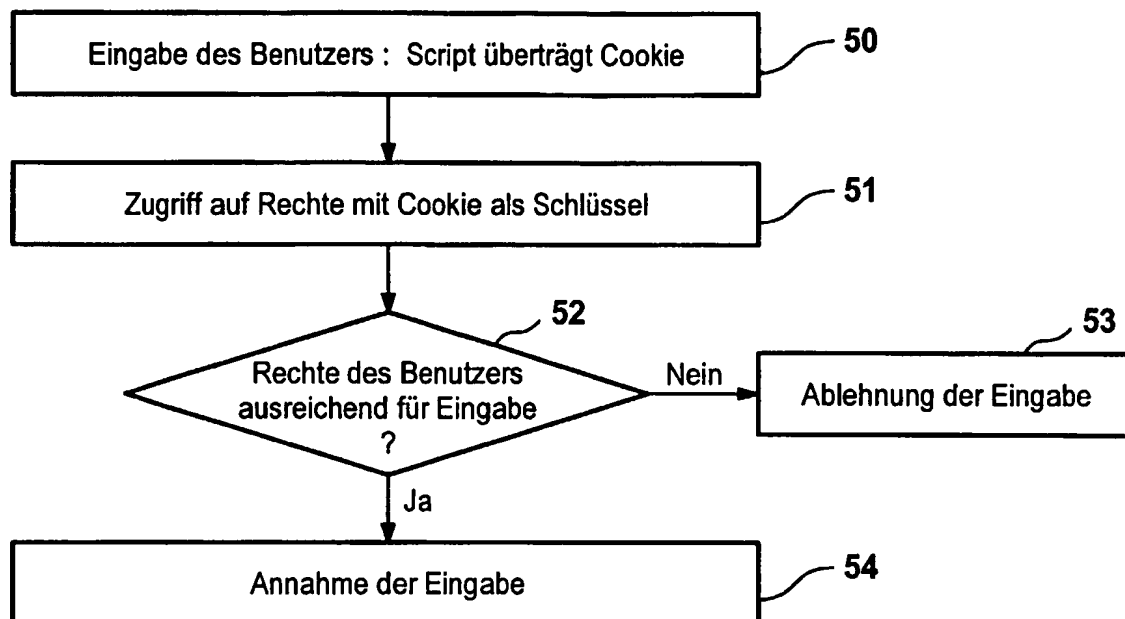


FIG 4

5 / 6

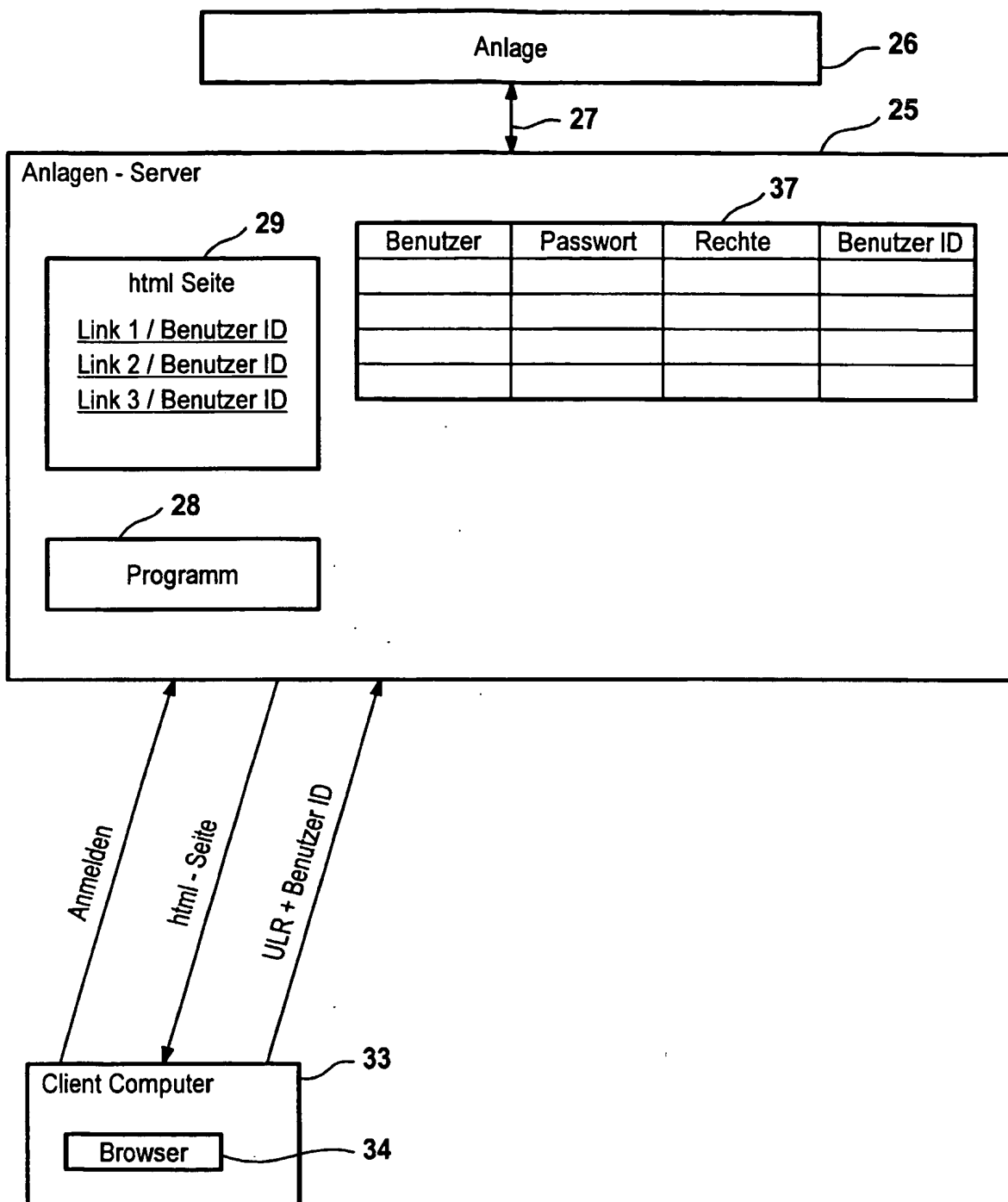


FIG 5

6 / 6

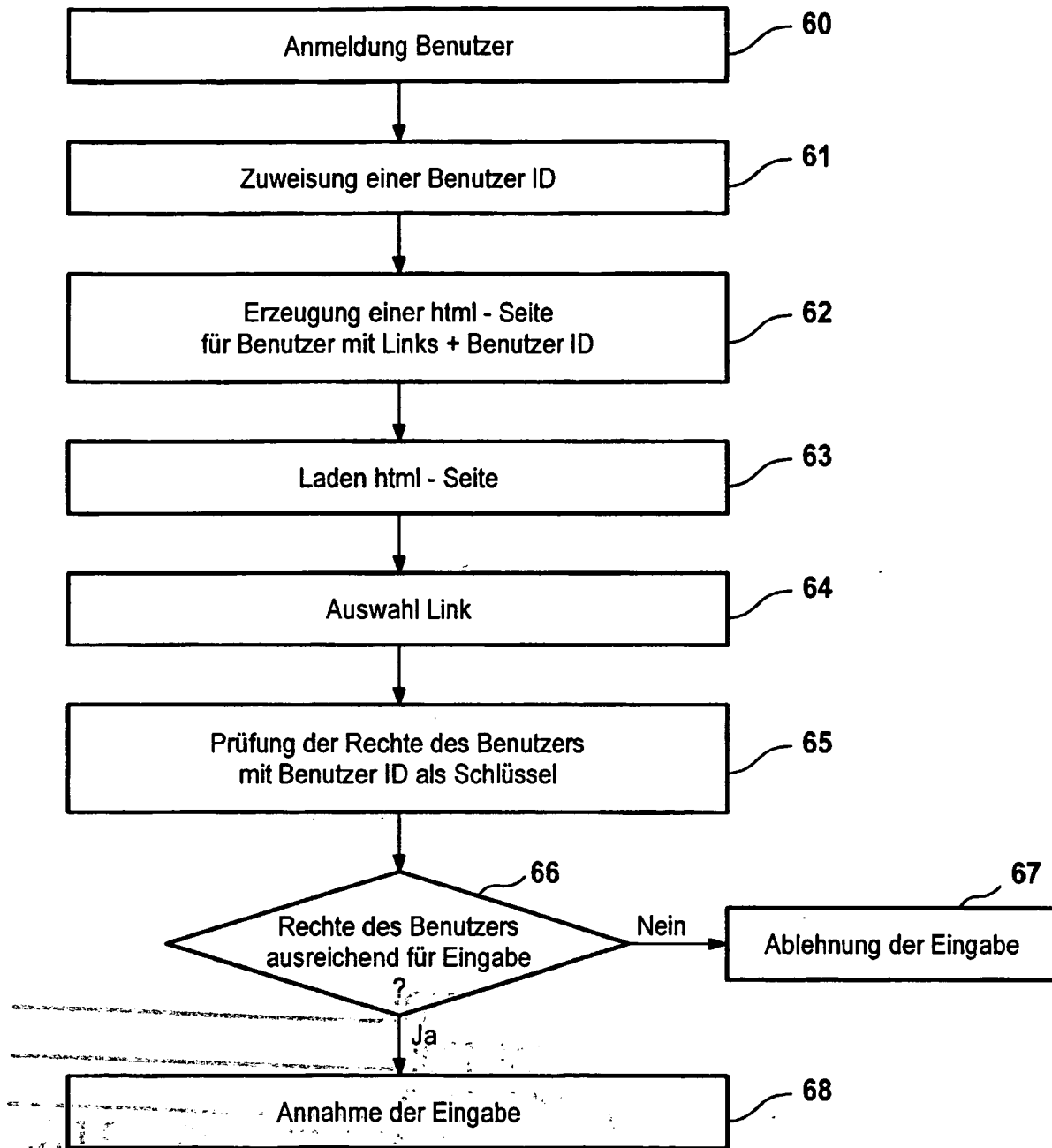


FIG 6